Non-Proprietary Security Policy for the FIPS 140-2 Level 1 Validated AirFortress™ Client Cryptographic Module Version 3.1

Document Revision 2.3
April 15, 2004

This security policy (Rev. 2.3) of Fortress Technologies, Inc., for the FIPS 140-2 validated AirFortress™ Client Cryptographic Module (AF Client), Version 3.1, defines general rules, regulations, and practices under which the AF Client was designed and developed and for its correct operation. These rules and regulations have been and must be followed in all phases of security projects, including the design, development, manufacture service, delivery and distribution, and operation of products.

Contents

Figures and Tables

1.0 INTRODUCTION

This security policy defines all security rules under which all products the AirFortress™ Client (AF Client) must operate and enforce, including rules from relevant standards such as FIPS. The AF Client complies with all FIPS 140-2 level 1 requirements.

The AF Client is a *cryptographic software application* that operates as a multi-chip standalone cryptographic module. The cryptographic boundary of the module is the compiled application executable. The physical boundary is the hardware platform, such as a typical PC or a Personal Digital Assistant (PDA), on which the AF Client is installed. The AF Client identifies network devices and encrypts and decrypts traffic transmitted to and from those devices.

The AF Client software and computer hardware combination operates as an *electronic encryption application* designed to prevent unauthorized access to data transferred across a wireless network. The AF Client encrypts and decrypts traffic transmitted on that network, protecting all clients "behind" it on a protected network. Only authorized personnel, such as the system administrator (cryptographic officer), can log into the module.

The AF Client operates at the datalink, (also known as Media Access Control (MAC)) layer of the Open Systems Interconnection (OSI) model as shown in Figure 1. Most of the security protocols are implemented without human intervention to prevent any chance of human error.

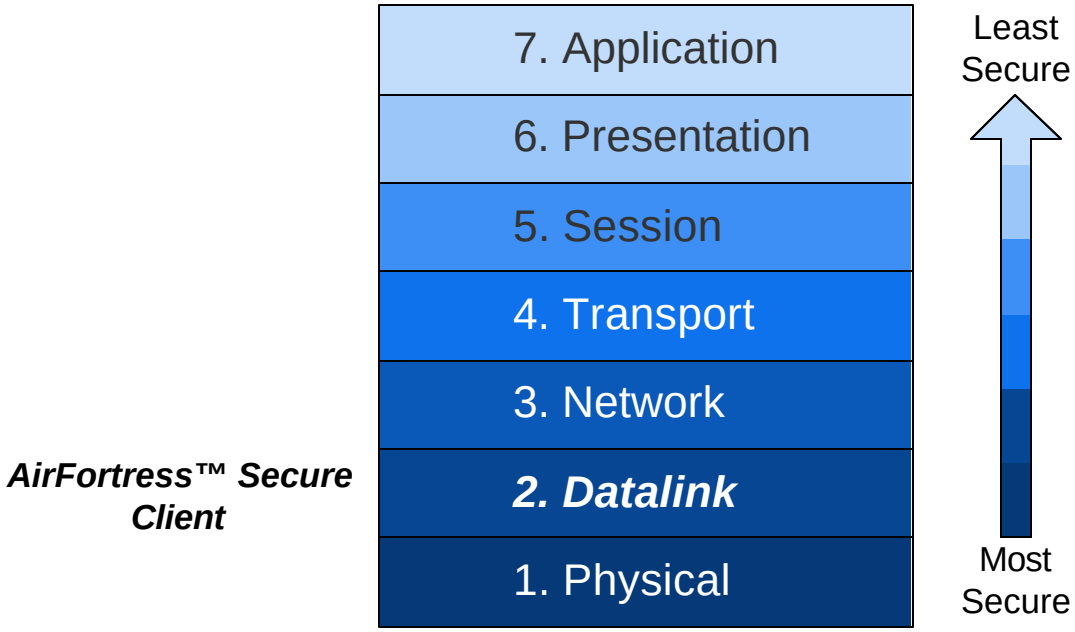

Figure 1: The Seven Layers of the OSI Reference Module

The AF Client is designed to operate on devices with Microsoft® Windows® 9x, NT, 2000, XP, and CE operating systems. Its security protocols are implemented without human intervention to prevent any chance of human error; therefore, the products operate with minimal intervention from the user. It secures communication within Local Area Networks (LANs), Wide Area Networks (WANs), and Wireless LANs (WLANs).

The cryptographic officer role manages the cryptographic configuration of the AF Client. Administrators can review module status and manage system settings where appropriate but not cryptographic settings when the modules are operating in FIPS mode. Because of the AF Client automates cryptographic processing, end users do not have to actively initiate cryptographic processing; the AF Client encrypts and decrypts data sent or received by users operating authenticated devices connected to the AF Client.

The AF Client offers point-to-point-encrypted communication between protected devices. Two or more AF Clients can communicate with each other directly or an AF Client can communicate to devices protected by an AirFortress™ Wireless Security Gateway. The products encrypt outgoing data from a client device and decrypt incoming data from networked computers located at different sites.

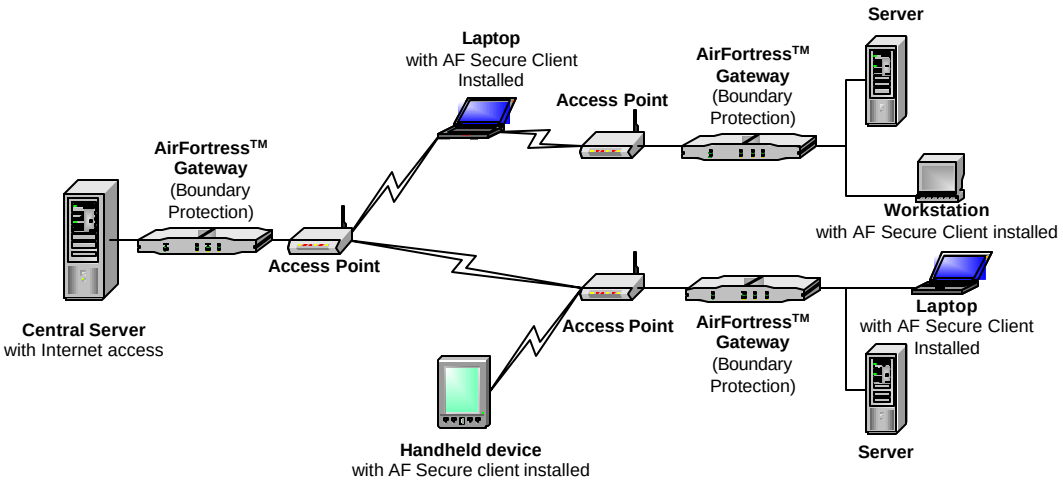

Figure 2: Example Configuration of AirFortress™ Client Deployment

2.0 AF CLIENT SECURITY FEATURES

The AF Client provides true datalink layer (Layer 2 in Figure) security. To accomplish this, it was designed with the minimum-security features described in the following sections.

2.1 Cryptographic Module

The following security design concepts guide the development of the AF Client:

1. Use strong, proven encryption solutions such as Triple DES (TDES), and AES.
2. Protect data at or below the level of vulnerability
3. Minimize the human intervention to the module operation with a high degree of automation to prevent human error and to ease the use and management of a security solution.
4. Secure all points where a LAN, WLAN, or WAN can be accessed by using a unique company Access ID, defined by the customer, to identify authorized devices as belonging to the protected wireless network

The Wireless Link Layer Security™ (wLLS) architecture of the cryptographic engine

ensures that cryptographic processing is secure on a wireless network and automates most security operations to prevent any chance of human error. Because wLLS operates at the datalink layer, header information is less likely to be intercepted. In addition to applying standard strong encryption algorithms, wLLS also compresses data, disguising the length of the data to prevent analytical attacks and yielding a significant performance gain on network throughput.

The AF Client requires no special configuration to operate once correctly installed by the cryptographic officer, although customers are encouraged to change certain security settings, such as the Access ID for the device, to ensure that each customer has unique parameters that must be met for access. The AF Client allows role-based access to user interfaces that access to the appropriate set of management and status monitoring tools.

2.2 Module Interfaces

The AF Client provides logical interfaces for input and output; it does not support separate ports for cryptographic key management or data authentication. Inbound and outbound traffic is received through the communication port of the hardware device on which the AF Client is installed. The information is processed by the Microsoft® Network Driver Interface Specification (NDIS) Intermediate protocol and then to the packet capture component, which identifies packets as incoming or outgoing and encrypts or decrypts the packets accordingly. This NDIS interface interacts with third-party applications installed on the computer that receives packets and with the device communication port (Network Interface Card (NIC), RJ-45 port, serial port, or other option).

Data sent and received through the NDIS interface to a connected access point are always encrypted; the AF Client does not allow plaintext transmission of data, cryptographic keys, or critical security parameters across a LAN or WLAN. Figure 3 shows this information flow in relation to a standard set of computer components that will be present on any platform on which the AF Client is installed.

The module has one logical interface for information flow, which handles all communication into and out of the module. Data is transmitted to the network exclusively as ciphertext. The AF Client does not require physically separate entry and exit ports. The device communications port serves as both a data entry and exit port for secured network communications, as the data streams are bi-directional and conform to the real-time information exchange over the network.

2.3 FIPS Mode

Each AF Client is configured by default to accept and send packets only as ciphertext. Only this way the Client can communicate with other secured AF modules.

The AF Client is a software application designed to be installed on a range of hardware devices that access a secured LAN or WLAN. According to FIPS 140-2 terminology, the AF Client is a multi-chip standalone cryptographic module, whose cryptographic boundary is the self-contained compiled executable.

.

The AF Client offers point-to-point-encrypted communication for the wireless electronic device it protects. It encrypts outgoing messages (data) from the device to the wired

network where an AirFortress™ Wireless Security Gateway is installed and decrypts incoming messages (data) to the host device from other devices within the AF Gateway-protected network. Two devices with AF Client installed and configured appropriately can also communicate with each other directly.

The AF Client units designed for government use apply FIPS-approved encryption algorithms, Triple Data Encryption Standard (TDES, Certification #19) and Advanced Encryption Standard (AES, Certification #14). These algorithms operate on text blocks of 64 bits and 128 bits, respectively, to encrypt and decrypt plaintext into ciphertext and ciphertext into plaintext. DES (FIPS Certificate #23) is also supported for legacy systems that require DES.

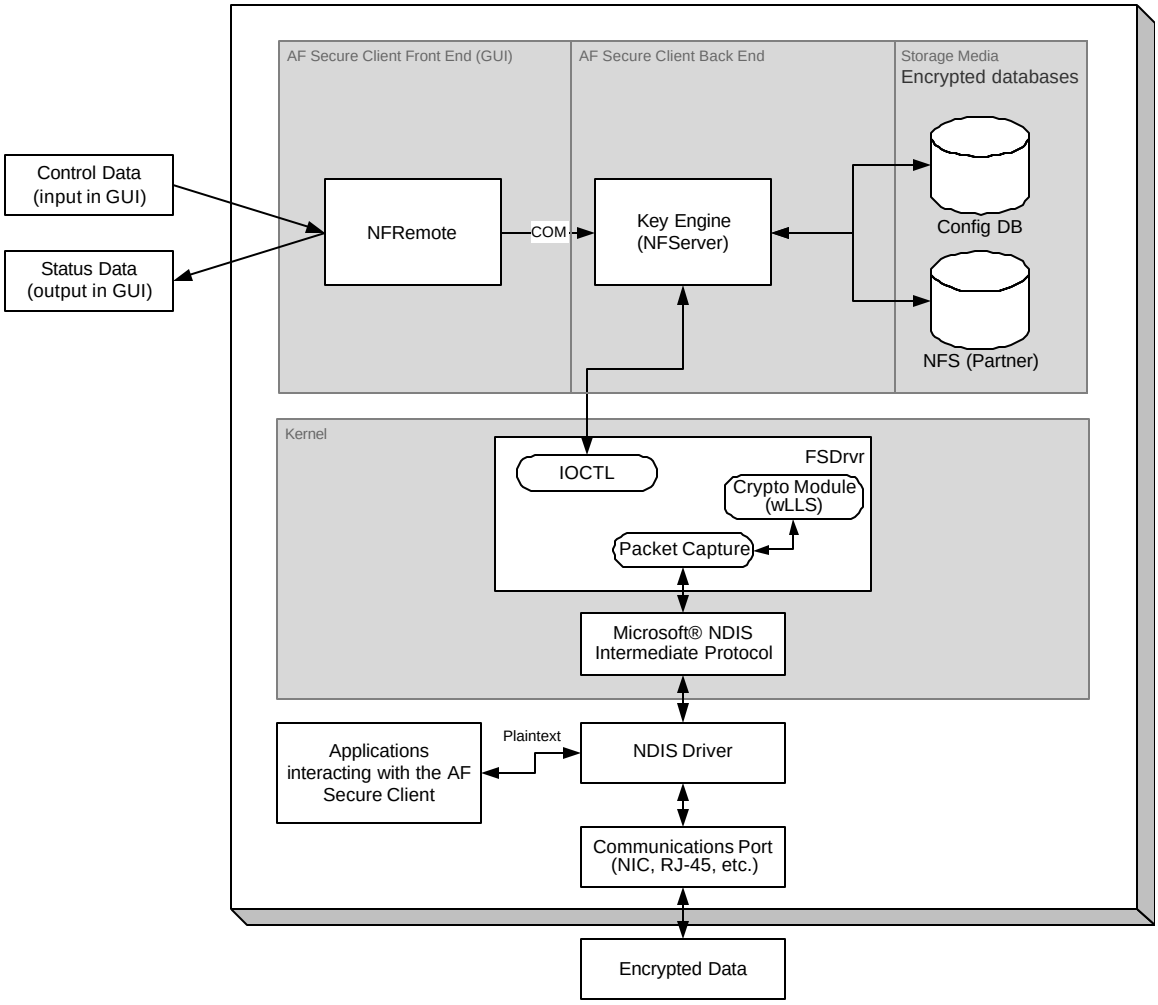

Figure 3: Information Flow Through the AF Client

3.0 IDENTIFICATION AND AUTHENTICATION POLICY

3.1 Roles

The AF Client supports two roles, the user roles and the cryptographic officer roles. Role based authentication is supported.

3.1.1 The User

The user role of the AF Client can monitor system status and perform the following tasks:

- Review system status information
- Turn encryption off (non-FIPS mode only)
- Toggle system messages on or off
- Reset current session keys (effectively zeroizing the session keys)
- Restart the AF Client

The user cannot change any critical system or cryptographic settings.

3.1.2 The Cryptographic Officer

The role assumed to perform a set of cryptographic initialization or management functions (e.g., module initialization, input/output of cryptographic keys and CSPs, and audit functions). The cryptographic officer performs the following tasks in particular:

- Install the AF Client
- Configure the unique access ID
- Import an access ID
- Select the cryptographic algorithm to use
- Set operation mode to FIPS or non-FIPS
- Configure cryptographic officer password
- Reset current session keys (effectively zeroizing the session keys)
- Create an emergency repair disk

The cryptographic officer performs most tasks while installing the AF Client. Access to other cryptographic controls after the product is installed requires the cryptographic officer to enter the correct password. Passwords must be of a minimum specified length.

3.2 Services

The following *key management* services are provided in the Client without requiring operator intervention:

- Generating the module's keys
- Generating cryptographic keys using encrypted Diffie-Hellman exchanges to prevent man-in-the-middle attacks
- Creating and maintaining tables (users can manually clear tables)

- Authenticating devices attempting to communicate with the AF Client
- Reinitiating key exchange at user-specified intervals
- Zeroizing keys if power to the module is turned off

The following *cryptographic operations* services are provided in the module without requiring operator intervention:

- Filtering packets to prevent any unencrypted (and, therefore, unauthorized) packets from entering the network
- Encrypting and decrypting packets at the datalink layer (OSI level 2)
- Authenticating the origin of packets
- Testing packet integrity using a SHA-1 hash

Other services performed by the module include monitoring and displaying device status and performing all self-tests.

The following tables show the services supported and allowed to the Cryptographic Officer and the User roles, also a Summary of Service provided by the SF Client product.

Table 1: Cryptographic Officer

Security Relevant Data Item	Show	Set	Save	Restore	Enable	Disable	Restart	Reset
Access ID		X						
Crypto keys								X
Cryptography algorithm	X	X						
Device ID	X		X	X				
Device MAC	X							
FIPS mode					X	X		
Role passwords		X						
Self Tests							X	

Table 2: User

Security Relevant Data Item	Show	Save	Restore	Restart	Reset
Access ID					
Crypto keys					X
Cryptography algorithm	X				

Security Relevant Data Item	Show	Save	Restore	Restart	Reset
Device ID	X	X	X		
Device MAC	X				
Cryptography algorithm	X				
FIPS mode	X				
Role passwords					
Self Tests				X	

Table 3: Summary of Cryptographic Services

Service	Input	Output	Role
Configure cryptographic officer password	Command	Password	CO
Configure the unique access ID	Command	ID	CO
Encryption	Plain text	Cipher text	User
Decryption	Cipher text	Plain text	User
Set Device MAC	Device ID	Device ID	CO
FIPS mode on/off	Command	Status	CO
Install/set-up the AF Client	Command	Configured AFC	CO
Key Management	None	Crypto keys	User
Select the cryptographic algorithm to use	Command	DES, TDES, AES	CO
Reset current session	Command	New status	CO, U
Review status	Command	Status	CO, U
Self-tests	Command	Status	CO, U

Note: CO- Cryptographic Officer, AFC- AirFortress™ Client, U-user

3.3 Self-Tests

The following list of all self-tests includes both power-up tests and conditional tests that apply to the AF Client.

A. Power-Up Tests

- Cryptographic Algorithm Test
  - ◊ AES KAT

- ◊ TDES KAT
- ◊ DES KAT
- ◊ HMAC-SHA-1 KAT
- ◊ SHA-1 KAT

- Software/Firmware Test, HMAC-SHA-1
- Critical Functions Test, None

B. Conditional Tests

- Continuous Random Number Generator test, Comparison with previous numbers first 8-byte block

4.0 CRYPTOGRAPHIC KEY MANAGEMENT

The AF Client itself automatically performs all cryptographic processing and key management functions.

4.1 Key Generation

The AF Client uses seven cryptographic keys, generated by FIPS-approved processes:

- Module's Secret Key (Symmetric, 3DES and AES)
- Static Private Key
- Static Public Key
- Static Secret Encryption Key (Symmetric, 3DES and AES)
- Dynamic Private Key
- Dynamic Public Key
- Dynamic Session Key (Symmetric, 3DES and AES)

Symmetric DES keys are used for backward compatibility with legacy units.

The public and private keys above are those used in the Diffie-Hellman key agreement protocol.

An ANSI X9.31 A.2.4 pseudo-random number generator generates random numbers used for generating the module private keys.

4.2 Key Storage

No encryption keys are stored permanently in the module hardware.

4.3 Zeroization of Keys

The session keys of the AF Client are automatically zeroized when the system is turned off and regenerated at every boot-up of the host hardware. All session keys can be zeroized manually by the crypto officer.

4.4 Protocol Support

The AF Client supports the Diffie-Hellman key agreement protocol

4.5 Cryptographic Algorithms

The AF Client applies the following cryptographic algorithms:

Table 4: Algorithms Supported by the AF Client

FIPS Algorithms	NIST Certificate number
AES (ECB, CBC, encrypt/decrypt; 128, 192, 256)	14
3DES (CBC, encrypt/decrypt)	19
DES (ECB, CBC, encrypt/decrypt)	23
SHA-1 (Byte)	34
HMAC-SHA-1	34 (Vendor affirmed)
Non-FIPS Algorithms	
Diffie-Hellman Key Agreement	None

5.0 ACCESS CONTROL POLICY

The AF Client allows role-based access to user interfaces that access to the appropriate set of management and status monitoring tools. Direct console access supports the majority of System Administrator (Cryptographic Officer) tasks.

Users can review module status and manage system settings where appropriate but not cryptographic settings when the modules are operating in FIPS mode. Because of the AF Client automates cryptographic processing, end users do not have to actively initiate cryptographic processing; the AF Client encrypts and decrypts data sent or received by users operating authenticated devices connected to the AF Client

The Crypto-Officer must use his/her password ID to access the system. The password can be defined with letters, numbers and special characters. It must be minimum eight (8) characters long. (The maximum length can be 72 character)

The Tables 1 and 2, defined by Fortress Technologies' Access Control Policy, show the authorized access and services supported and allowed to each role. As a user does not have any interaction with the module security relevant data items.

6.0 PHYSICAL SECURITY POLICY

The AF Client was designed to be installed on production quality devices as defined by the FIPS PUB 140-2 for security level 1. However, as the AF Client is delivered as a software cryptographic module only, the physical security requirements do not apply to the module.

The AF Client was tested on the following operating system/hardware combinations:

Windows 2000

Pentium III 450 MHz

256 MB DRAM

8 GB IDE Hard-drive

CD, 1.44 MB Floppy Drive

Netgear 10/100 Mbps NIC

Generic 8 MB Video Accelerator Display Card

MS DOS 6.20, Windows 9x & Windows NT 4.0

Multiboot system

Pentium II 266 MHz

64 MB RAM

6.5 MB HD Total

CDROM, 1.44 MB Floppy Drive

Generic 10/100 Mbps NIC

Generic VGA Display Card

Windows XP

Pentium IV 1.60 GHz

256 MB RAM

17 GB IDE HD

CD, 1.44 MB Floppy Drive

Netgear 10/100 Mbps NIC

Generic SVGA Display Card

Windows CE 3.0

Compaq iPaq pocket pc

ARM SA1110

64 MB RAM

Compaq WL110 11 Mbps Wireless LAN NIC

5V Power & Battery (120 to 5 volt converter included)

PalmOS 4.1

Symbol Module Number SPT1846 1D

4 MB Fijitsu FLASH

8 MB RAM

11 Mbps T2 S24 Wireless LAN NIC

4.05V Power & Battery (120 to 4.05 converter included)

The physical security of a deployed AF Client is determined by the customer's security policy.

7.0 SOFTWARE SECURITY

The AF Client software is written in C and C++ and operates on most versions of the Windows operating system. The software is installed in the host hardware storage medium as a compiled executable.

Self-tests validate the operational status of each product, including critical functions and files. If the software is compromised, the module enters an error state in which no cryptographic processing occurs, preventing a security breach through a malfunctioning device.

8.0 OPERATING SYSTEM SECURITY

The AF Client operates on Microsoft® Windows® 95, 98, NT, 2000, XP, CE, and PalmOS. The operating system must be in single-user mode. The AF Client operates automatically after power-up.

9.0 MITIGATION OF OTHER ATTACKS POLICY

No special mechanisms are built in the AF Client; however, the cryptographic module is designed to mitigate several specific attacks. Features, which mitigate attacks, are listed here:

1. Use of a network-specific *access ID* assures that only AF Client units using this same unique value can establish key exchange: *Mitigates unauthorized connections to the module.*
2. The AF Client uses FIPS-approved SHA-1 and HMAC-SHA-1 hashing (NIST certification #34) and FIPS-approved encryption/decryption methods: DES (certification #23), 3DES (certification #23), AES (certification # 14): *Mitigates attacks to decrypt traffic and crack keys*.
3. The AF Client enforces strong authentication of communicating parties: *Mitigates "spoofing" credentials*.
4. The AF Client applies strong authentication of the origin of the packets: *Mitigates packet modification.*
5. The dynamic session key is changed at least once every 24 hours, with 4 hours being the factory default duration: *Mitigates key discovery.*
6. A second Diffie-Hellman key exchange produces a dynamic common secret key in each of the modules by combining the other module's dynamic public key with the module's own dynamic private key: *Mitigates "man-in-the-middle" attacks.*
7. All key exchanges are encrypted: *Mitigates encryption key sniffing by hackers.*
8. Data in transit is subjected to integrity checking: *Mitigates data modification and active attacks to inject traffic*.
9. Compression and encryption of header information inside of the frame, making it impossible to guess. Use of strong encryption further protects the information. Any bit flipping would be useless in this frame to try to change the IP address of the frame: *Mitigates active attacks from both ends*.
10. The AF Client passes only encrypted communication and does not support plaintext communication: All data packets sent over a LAN or WLAN are

encrypted: *Mitigates unauthorized access to the sent data.*

11. Encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*
12. No encryption keys are stored permanently in the module: *Mitigates key discovery.*
13. All software data are stored in executable format in the module: *Mitigates access to the module software.*
14. When the AF Client is operated in accordance to the vendor's physical security policy, the host server hardware platform is located in a controlled-access area or under permanent control of the user: *Mitigates access to the module hardware.*

10.0 EMI/EMC

The Fortress Technologies, Inc.'s engineer or the customer's cryptographic officer installs the AF Client on FCC-compliant (Part 15, Subpart J, Class A), Class B devices.

11.0 CUSTOMER SECURITY POLICY ISSUES

FTI expects that after the module's installation, any potential *customer* (government organization or commercial entity or division) *employs its own internal security policy* covering all the rules under which the module(s) and the customer's network(s) must operate. In addition, the customer systems are expected to be upgraded as needed to contain appropriate security tools to enforce the internal security policy.

12.0 MAINTENANCE ISSUES

All software installation and reinstallation for modules is performed by the cryptographic officer following the procedures defined by Fortress Technologies. Software troubleshooting to resolve an error state may require the product to be reinstalled by the cryptographic officer.

- * - * -

End of the "Non-Proprietary Security Policy for the FIPS 140-2 Validated AirFortress™ Client Cryptographic Module" document.